PCT/JP00/03838

EU

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 ３月 ３日

出願番号
Application Number: 特願２０００－０５９３６９

出願人
Applicant (s): 株式会社エヌ・ティ・ティ・ドコモ

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年 ７月２１日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０５７５２１

【書類名】　特許願
【整理番号】　DCMH110353
【提出日】　平成12年 3月 3日
【あて先】　特許庁長官　殿
【国際特許分類】　G11C 7/00
【発明の名称】　メモリデバイス
【請求項の数】　12
【発明者】
【住所又は居所】　東京都港区虎ノ門二丁目１０番１号　エヌ・ティ・ティ移動通信網株式会社内
【氏名】　福本　雅朗
【発明者】
【住所又は居所】　東京都港区虎ノ門二丁目１０番１号　エヌ・ティ・ティ移動通信網株式会社内
【氏名】　杉村　利明
【特許出願人】
【識別番号】　392026693
【住所又は居所】　東京都港区虎ノ門二丁目１０番１号
【氏名又は名称】　エヌ・ティ・ティ移動通信網株式会社
【代理人】
【識別番号】　100098084
【弁理士】
【氏名又は名称】　川△崎▽　研二
【選任した代理人】
【識別番号】　100111763
【弁理士】
【氏名又は名称】　松本　隆
【選任した代理人】
【識別番号】　100108936

【弁理士】

【氏名又は名称】　秦　貴清

【手数料の表示】

【予納台帳番号】　038265

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　メモリデバイス

【特許請求の範囲】

【請求項１】　利用側ユニットに利用されるメモリデバイスであって、

前記利用側ユニット側から通常のファイルアクセス方法にて読み書き可能な汎用記憶部と、前記利用側ユニット側から前記通常のファイルアクセス方法にて書き込み可能な書き込み専用領域と、ユーザの本人認証の基準となる登録データを前記利用側ユニット側からアクセス不可能に格納した登録領域とを有する記憶手段と、

前記利用側ユニット側から前記書き込み専用領域へユーザの入力データが書き込まれると、該入力データと前記登録データとが所定の関係を満たすか否かを判別する認証処理を行い、満たすと判別された場合にのみ、自デバイスの状態を前記利用側ユニット側から前記汎用記憶部へのアクセスを許容した状態とする認証制御手段と

を具備することを特徴とするメモリデバイス。

【請求項２】　前記利用側ユニットに対して着脱され、

前記利用側ユニットへの自デバイスの装着を検知する装着検知手段を具備し、

前記認証制御手段は、前記装着検知手段によって前記利用側ユニットへの自デバイスの装着が検知され、かつ前記利用側ユニット側から前記書き込み専用領域へユーザの入力データが書き込まれると、前記認証処理を行う

ことを特徴とする請求項１に記載のメモリデバイス。

【請求項３】　前記利用側ユニットへのユーザのログインを検知するログイン検知手段を具備し、

前記認証制御手段は、前記ログイン検知手段によって前記利用側ユニットへのユーザのログインが検知され、かつ前記利用側ユニット側から前記書き込み専用領域へユーザの入力データが書き込まれると、前記認証処理を行う

ことを特徴とする請求項１に記載のメモリデバイス。

【請求項４】　前記認証制御手段は、前記書き込み専用領域への所定回数以下の書き込みのみを前記利用側ユニットに許容し、前記所定回数以下の書き込み

において前記認証処理の判別結果が前記所定の関係を満たす旨の結果となった場合にのみ、自デバイスの状態を前記利用側ユニット側から前記汎用記憶部へのアクセスを許容した状態とする

ことを特徴とする請求項１乃至３のいずれかに記載のメモリデバイス。

【請求項５】　前記認証制御手段は、さらに、前記所定回数以下の書き込みにおいて前記認証処理の判別結果が一度も前記所定の関係を満たす旨の結果とならなかった場合には、自デバイスの状態を前記利用側ユニット側から前記書き込み専用領域への書き込みを禁止した状態とする

ことを特徴とする請求項４に記載のメモリデバイス。

【請求項６】　前記入力データはユーザが入力したパスワードを表すデータであり、前記登録データは正しいパスワードを表すデータであり、前記所定の関係は一致関係であることを特徴とする請求項１乃至３のいずれかに記載のメモリデバイス。

【請求項７】　前記認証制御手段は、自デバイスが前記利用側ユニットから離脱すると自デバイスの状態を前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容した状態とする

ことを特徴とする請求項２に記載のメモリデバイス。

【請求項８】　前記認証制御手段は、ユーザが前記利用側ユニットに対してログアウトすると自デバイスの状態を前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容した状態とする

ことを特徴とする請求項３に記載のメモリデバイス。

【請求項９】　前記認証制御手段は、さらに、前記認証処理の後に、前記利用側ユニットに対する自デバイスの着脱状態の変化を擬似的に表わす信号を前記利用側ユニットへ出力する

ことを特徴とする請求項２に記載のメモリデバイス。

【請求項１０】　前記認証制御手段は、さらに、前記利用側ユニット側から特定の指示を受け取ると、自デバイスの状態を、前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容し、かつ前記装着検知手段によって前記利用側ユニットへの自デバイスの装着が検知された状態とする

ことを特徴とする請求項２に記載のメモリデバイス。

【請求項１１】　前記認証制御手段は、さらに、前記利用側ユニット側から特定の指示を受け取ると、自デバイスの状態を、前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容し、かつ前記ログイン検知手段によって前記利用側ユニットへのユーザのログインが検知された状態とする

ことを特徴とする請求項３に記載のメモリデバイス。

【請求項１２】　前記認証制御手段は、さらに、前記利用側ユニット側から前記書き込み専用領域を前記通常のファイルアクセス方法にて読み出す要求を受け取ると、自デバイスの状態を表す情報を返送する

ことを特徴とする請求項１乃至３のいずれかに記載のメモリデバイス。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ユーザデータを保管可能なメモリデバイス（記憶装置）に関する。

【０００２】

【従来の技術】

近年、コンピュータを利用した様々なサービスが日々、開発・提供されている。この種のサービスには、電子メールや電子商取引、オンラインでの銀行取引などのサービスも含まれており、他者への漏洩を回避する必要のある個人情報がコンピュータのメモリデバイス（例えばハードディスク）に保管される可能性が高くなってきている。このことは不揮発性の半導体メモリ（あるいはバッテリバックアップされた揮発性の半導体メモリ）や小型のハードディスク等を内蔵したＰＣカードのような、着脱式のメモリデバイスにも共通しており、個人情報のセキュリティの確保が重要になってきている。

【０００３】

特にＰＣカード等の着脱可能なメモリデバイスは携帯性に優れており、かつ様々なコンピュータに装着可能な汎用性を備えているため、ハードディスク等のコンピュータに固定的に内蔵されるデバイスに比較して単体で携行されることが多く、紛失の可能性を排除することは不可能である。すなわち、個人情報を保管し

たメモリデバイスが他者の手に渡ることは有り得ることであり、セキュリティを確保するためには、メモリデバイスの使用時においてユーザの本人認証を行う必要がある。

【０００４】

カードを使用する使用者の本人認証方法としては、磁気ストライプを有するカード（例えばキャッシュカード）等については、暗証番号を入力する方法が知られている。また、認証データを記憶させたＩＣカード等については、当該認証データを読み取ってカギ情報を作成し、システム側に認証を求める方法が知られている。また、キャッシュレスサービス等では、より高いレベルでのセキュリティ確保を目的として、生体情報を用いた本人認証方法も提案されている。

【０００５】

【発明が解決しようとする課題】

しかしながら、従来の本人認証方法によれば、カードの利用の度に、カード上の磁気ストライプやカード内の認証データ等を読取装置に読み込ませたり、指紋情報等の生態情報を指紋認証装置等に読み取らせる必要がある。すなわち、カードが本来有する機能とは全く異なる特殊機能を用いた処理が必要となり、特に当該カードを利用する可能性のあるコンピュータ等の情報処理装置において、上記特殊機能を実現するためのハードウェア及びソフトウェアを用意しておかなければならないという欠点がある。この欠点は、ハードディスク等のコンピュータに固定的に内蔵されるメモリデバイスの利用に上記本人認証方法を適用した場合にも共通している。

【０００６】

本発明は上述した事情に鑑みて為されたものであり、メモリデバイスを利用する利用側ユニット側に何ら変更を加えることなく個人情報等のユーザデータのセキュリティを確保することができるメモリデバイスを提供することを目的としている。

【０００７】

【課題を解決するための手段】

上記課題を解決するため、請求項１記載の発明は、利用側ユニットに利用され

るメモリデバイスであって、

前記利用側ユニット側から通常のファイルアクセス方法にて読み書き可能な汎用記憶部と、前記利用側ユニット側から前記通常のファイルアクセス方法にて書き込み可能な書き込み専用領域と、ユーザの本人認証の基準となる登録データを前記利用側ユニット側からアクセス不可能に格納した登録領域とを有する記憶手段と、

前記利用側ユニット側から前記書き込み専用領域へユーザの入力データが書き込まれると、該入力データと前記登録データとが所定の関係を満たすか否かを判別する認証処理を行い、満たすと判別された場合にのみ、自デバイスの状態を前記利用側ユニット側から前記汎用記憶部へのアクセスを許容した状態とする認証制御手段とを具備することを特徴としている。

このメモリデバイスでは、利用側ユニット側から書き込み専用領域へ入力データが書き込まれると、この入力データに基づいてユーザの本人認証が行われる。そして、ユーザの本人性が認証された場合にのみ、利用側ユニットからメモリデバイスの汎用記憶部へのアクセスが可能となる。

【０００８】

また、請求項２記載の発明は、請求項１記載のメモリデバイスにおいて、前記利用側ユニットに対して着脱され、

前記利用側ユニットへの自デバイスの装着を検知する装着検知手段を具備し、

前記認証制御手段は、前記装着検知手段によって前記利用側ユニットへの自デバイスの装着が検知され、かつ前記利用側ユニット側から前記書き込み専用領域へユーザの入力データが書き込まれると、前記認証処理を行うことを特徴としている。

このメモリデバイスによれば、ユーザの本人認証が、メモリデバイスの利用者ユニットへの装着時に行われる。

【０００９】

さらに、請求項３記載の発明は、請求項１記載のメモリデバイスにおいて、

前記利用側ユニットへのユーザのログインを検知するログイン検知手段を具備し、

前記認証制御手段は、前記ログイン検知手段によって前記利用側ユニットへのユーザのログインが検知され、かつ前記利用側ユニット側から前記書き込み専用領域へユーザの入力データが書き込まれると、前記認証処理を行うことを特徴としている。

このメモリデバイスによれば、ユーザの本人認証が、利用側ユニットに対するユーザのログイン時に行われる。

【００１０】

また、請求項４記載の発明は、請求項１乃至３のいずれかに記載のメモリデバイスにおいて、前記認証制御手段は、前記書き込み専用領域への所定回数以下の書き込みのみを前記利用側ユニットに許容し、前記所定回数以下の書き込みにおいて前記認証処理の判別結果が前記所定の関係を満たす旨の結果となった場合にのみ、自デバイスの状態を前記利用側ユニット側から前記汎用記憶部へのアクセスを許容した状態とすることを特徴としている。

このメモリデバイスによれば、書き込み専用領域への所定回以下の書き込みが許容される。

【００１１】

さらに、請求項５記載の発明は、請求項４記載のメモリデバイスにおいて、前記認証制御手段は、さらに、前記所定回数以下の書き込みにおいて前記認証処理の判別結果が一度も前記所定の関係を満たす旨の結果とならなかった場合には、自デバイスの状態を前記利用側ユニット側から前記書き込み専用領域への書き込みを禁止した状態とすることを特徴としている。

このメモリデバイスによれば、所定回の書き込みにおいても正しい入力データが書き込まれない場合には利用側ユニットから書き込み専用領域への書き込み自体が禁止される。

【００１２】

また、請求項６記載の発明は、請求項１乃至３のいずれかに記載のメモリデバイスにおいて、前記入力データはユーザが入力したパスワードを表すデータであり、前記登録データは正しいパスワードを表すデータであり、前記所定の関係は一致関係であることを特徴としている。

【００１３】

さらに、請求項７記載の発明は、請求項２記載のメモリデバイスにおいて、前記認証制御手段は、自デバイスが前記利用側ユニットから離脱すると自デバイスの状態を前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容した状態とすることを特徴としている。

このメモリデバイスでは、利用側ユニットへの自デバイスの再装着時に、自デバイスの状態が、利用側ユニット側から前記書き込み専用領域への書き込み以外のアクセスを禁止した状態となる。

【００１４】

また、請求項８記載の発明は、請求項３記載のメモリデバイスにおいて、前記認証制御手段は、ユーザが前記利用側ユニットに対してログアウトすると自デバイスの状態を前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容した状態とすることを特徴としている。

このメモリデバイスでは、利用側ユニットに対するユーザの再ログイン時に、自デバイスの状態が、利用側ユニット側から前記書き込み専用領域への書き込み以外のアクセスを禁止した状態となる。

【００１５】

さらに、請求項９記載の発明は、請求項２記載のメモリデバイスにおいて、前記認証制御手段は、さらに、前記認証処理の後に、前記利用側ユニットに対する自デバイスの着脱状態の変化を擬似的に表わす信号を前記利用側ユニットへ出力することを特徴としている。

この信号を受け取った利用側ユニットでは、メモリデバイスの着脱状態が変化したものと解釈される。

【００１６】

また、請求項１０記載の発明は、請求項２記載のメモリデバイスにおいて、前記認証制御手段は、さらに、前記利用側ユニット側から特定の指示を受け取ると、自デバイスの状態を、前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容し、かつ前記装着検知手段によって前記利用側ユニットへの自デバイスの装着が検知された状態とすることを特徴としている。

このメモリデバイスによれば、再装着を行わずとも、認証処理が開始される。

【００１７】

さらに、請求項１１記載の発明は、請求項３記載のメモリデバイスにおいて、前記認証制御手段は、さらに、前記利用側ユニット側から特定の指示を受け取ると、自デバイスの状態を、前記利用側ユニット側から前記書き込み専用領域への書き込みのみを許容し、かつ前記ログイン検知手段によって前記利用側ユニットへのユーザのログインが検知された状態とすることを特徴としている。

このメモリデバイスによれば、再ログインを行わずとも、認証処理が開始される。

【００１８】

また、請求項１２記載の発明は、請求項１乃至３のいずれかに記載のメモリデバイスにおいて、前記認証制御手段は、さらに、前記利用側ユニット側から前記書き込み専用領域を前記通常のファイルアクセス方法にて読み出す要求を受け取ると、自デバイスの状態を表す情報を返送することを特徴としている。

このメモリデバイスによれば、利用側ユニットからの通常のファイルアクセス方法によるファイルアクセスの応答として自デバイスの状態が返送される。

【００１９】

【発明の実施の形態】

以下、本発明の好ましい実施形態について図面を参照しつつ説明する。

【００２０】

Ａ．第１実施形態

まず、本発明の第１実施形態について説明する。

【００２１】

Ａ－１．基本的技術思想

まず、本実施形態において採用された基本的技術思想について説明する。

本実施形態では、着脱式のメモリデバイスを対象としており、メモリデバイス内にユーザデータを記憶するための汎用メモリ領域と本人認証および自デバイスの動作の制御を行う手段とを設けている。そして、本実施形態に係るメモリデバイスは、利用側ユニットへの自デバイスの装着時には、自デバイスの認証ステー

タスを、自デバイス内の書き込み専用ファイルへの書き込みのみを利用側ユニットに対して許容する準備未完了ステータスとし、この書き込み専用ファイルにパスワードとして利用側ユニット側から書き込まれたデータとメモリデバイス内に予め登録されたデータ（利用側ユニットから読み出し不可能に格納されたデータ）とを比較し、両者が一致した場合にのみ、自デバイスの認証ステータスを、利用側ユニット側から汎用メモリ領域へのアクセスを許容する準備完了ステータスへ変更するようにしている。

【００２２】

Ａ－２．システム構成

まず、本実施形態に係るメモリデバイスを用いた認証システムの構成について説明する。図１は本実施形態に係るメモリデバイスを用いた認証システムの構成を示すブロック図であり、図２は同メモリデバイスにおける認証処理の流れを示すフローチャートである。図１において、１は不揮発性のメモリデバイスとして機能するＰＣカード、６はＰＣカード１を装着するためのＰＣカードスロットを有する利用側ユニットであり、ＰＣカードスロットに装着されたＰＣカード１をメモリデバイスとして利用する。

【００２３】

本実施形態では、利用側ユニット６として一般的なＯＳ（オペレーティングシステム）を搭載した携帯型コンピュータを想定しているが、ＰＣカードスロットを有し、かつ一般的なＯＳを搭載していれば、据置型のコンピュータやデジタルカメラ等の各種の電子機器であってもよい。

【００２４】

利用側ユニット６は、ＰＣカードスロットに装着されたＰＣカード１の認証ステータスが準備未完了ステータスとなると、このＰＣカード１を利用するためのパスワードの入力を促すユーザインタフェースをユーザに提供する。また、ユーザが当該ユーザインタフェースを用いてパスワードを入力すると、当該パスワードを表すパスワード入力データを上記ＯＳの通常のファイルアクセス方法によりＰＣカード１内の所定のファイル（後述の書き込み専用ファイル２ｃ）に書き込む。

【００２５】

また、利用側ユニット６は、ＰＣカードスロットに装着されたＰＣカード１内の書き込み専用ファイル２ｃを通常のファイルアクセス方法により読み出そうとしたときにＰＣカード１側から供給されるステータス文字列（ＰＣカード１の認証ステータスを表す文字列）をユーザに通知する。

【００２６】

Ａ－３：ハードウェア構成

次に、ＰＣカード１のハードウェア構成について説明する。

図示を略すが、ＰＣカード１は、クレジットカード型の平面形状を有する所定厚さの筐体と、この筐体の端部に形成された所定形式（例えばＰＣカード・スタンダード（PC Card Standard）形式）の外部コネクタとを有している。この外部コネクタは利用側ユニット６との接続に用いられるものであり、汎用性が十分に高ければ、他の規格（例えばコンパクトフラッシュ（Compact Flash）・タイプII）に準拠したコネクタであってもよい。コンパクトフラッシュ・タイプのコネクタは通常のＰＣカード・スタンダードのものより小型（例えば、タイプIIは縦横が４２．８×３６．４（mm）、厚さが５．０（mm））であり、これを外部コネクタとして採用すれば、認証システムの小型化を図ることができる。なお、ＰＣカード・スタンダードとは、JEIDA（Japan Electronics Industry Development Association：日本電子工業振興協会）と米国PCMCIA（Personal Computer Memory Card International Association）が共同で制定した規格であり、カードの厚さ毎に異なるタイプI～タイプIVが規定されている。

【００２７】

また、ＰＣカード１は不揮発性の半導体メモリを備えている。なお、不揮発性の半導体メモリはバッテリバックアップされた揮発性の半導体メモリであってもよいし、小型のハードディスクであってもよい。

【００２８】

さらに、ＰＣカード１は外部コネクタを含む外部インタフェースと、この外部インタフェースを介して利用側ユニット６と接続されるマイクロコントローラとを備えている。このマイクロコントローラはＰＣカード１の動作を制御するもの

であり、例えば、半導体メモリに対するデータの書き込み／読み出し、外部インタフェースを介した利用側ユニット６とのデータの授受、および後述する各種処理などを行う。なお、本実施形態においては、ＰＣカード１内に電源が存在し、マイクロコントローラはこの内部電源からの電力供給を受けて作動する。

〔００２９〕

Ａ－４：機能構成

次に、上記ハードウェア構成上に実現されるＰＣカード１の機能構成について図１を参照して説明する。

図１に示すように、ＰＣカード１は、不揮発性メモリから構成された記憶手段２と、マイクロコントローラにより実現される認証処理手段３と、外部インタフェース及びマイクロコントローラにより実現される着脱検知手段（装着検知手段）４と、外部インタフェース及びマイクロコントローラにより実現される動作制御手段５とを有する。なお、認証処理手段３及び動作制御手段５は認証制御手段を構成している。

〔００３０〕

（１）記憶手段２

記憶手段２はユーザデータ等の情報を記憶するための手段であり、動作制御手段５により制御される。この記憶手段２は、ユーザデータを格納するための汎用メモリ領域（汎用記憶部）２ａとユーザの本人認証のための認証用データを格納するための認証用データ格納領域２ｂとから構成されている。前者の汎用メモリ領域２ａは、利用側ユニット６から通常のファイルアクセス方法にてアクセス可能となるように構成されており、後者の認証用データ格納領域２ｂには、上記通常のファイルアクセス方法でのデータの書き込みが許容された書き込み専用ファイル（書き込み専用領域）２ｃと、利用側ユニット６側からのアクセスが不可能な登録データファイル（登録領域）２ｄとが設けられている。

〔００３１〕

通常のファイルアクセス方法で書き込み可能な書き込み専用ファイル２ｃは、利用側ユニット６側からパスワードとして入力されたデータ（以後、パスワード入力データ（入力データ））が書き込まれるファイルであり、利用側ユニット６

側からは記憶手段２内のファイルの一つ（例えば、記憶手段２のルートディレクトリ内の“PASSWORD.DAT”というファイル名のファイル）として認識される。

【００３２】

登録データファイル２ｄはパスワード入力データと比較される登録パスワードデータ（登録データ）を格納したファイルであり、動作制御手段５にのみ読み出され得る。なお、利用側ユニット６側から登録データファイル２ｄへのアクセスは不可能であるため、利用側ユニット６側からは登録データファイル２ｄを使用することはもちろん、これを認識することもできない。

【００３３】

（２）着脱検知手段４

着脱検知手段４は、利用側ユニット６に対する自ＰＣカード１の着脱を検知し、動作制御手段５へ通知する。具体的には、利用側ユニット６との間の所定の接続信号ＣＤ＃１，ＣＤ＃２（標準ＰＣカードなら３６番ピン及び６７番ピン、コンパクトフラッシュカードなら２５番ピン及び２６番ピンに対応する信号）を監視することで着脱を検知する。

【００３４】

（３）認証処理手段３

認証処理手段３は、利用側ユニット６側からＰＣカード１へ入力されたパスワード入力データと予め登録された登録パスワードデータとに基づいてパスワードの比較を行う。具体的には、認証処理手段３は、動作制御手段５から所定の指示を受け取ると、書き込み専用ファイル２ｃに書き込まれた最新のパスワード入力データを読み出して登録データファイル２ｄに予め登録された登録パスワードデータと比較し、比較結果を動作制御手段５へ供給する。

【００３５】

（４）動作制御手段５

動作制御手段５は、ＰＣカード１の挙動を制御するものであり、基本的には、利用側ユニット６と記憶手段２との間のデータ授受を制御する。また、動作制御手段５は、着脱検知手段４の検知結果（利用側ユニット６に対するＰＣカード１の装着／離脱）および認証処理手段３の比較結果（パスワードの一致／不一致）

に応じた各種処理を行うとともに、利用側ユニット６からの書き込み専用ファイル２ｃの読み出し要求に応答して現在のＰＣカード１の認証ステータスを表すステータス文字列を返送する。以下、動作制御手段５が行う上記各種処理を分類して説明する。

【００３６】

①装着処理

着脱検知手段４によってＰＣカード１の利用側ユニット６への装着が検知されると、動作制御手段５は、ＰＣカード１の認証ステータスを、利用側ユニット６からの書き込み専用ファイル２ｃへの書き込みのみを許容する準備未完了ステータス（ステータス文字列“NOT READY”で表されるステータス）とするとともに、利用側ユニット６側から書き込み専用ファイル２ｃへのパスワード入力データの書き込み回数のカウントを開始する（初期値は０）。このカウント処理は後述の離脱処理（あるいは擬似離脱処理）が行われるまで継続される。なお、認証ステータスを変更するということは、ＰＣカード１の各部を変更後の認証ステータスで表される状態とすることを意味している。

【００３７】

②認証処理

また、ＰＣカード１の認証ステータスが準備未完了ステータスのときに、利用側ユニット６側からＰＣカード１側へパスワード入力データが書き込まれると、カウント値を１だけ増加させるとともに、認証処理手段３へ所定の指示を供給し、パスワードの比較を指示する。この比較結果がパスワード入力データと登録パスワードデータとの「一致」を示す場合には、動作制御手段５は、ＰＣカード１の認証ステータスを、記憶手段２の汎用メモリ領域２ａ内の各種ディレクトリやファイルを利用側ユニット６側から読み出し及び書き込み可能な準備完了ステータス（ステータス文字列“READY”で表されるステータス）とする。

【００３８】

逆に、当該比較結果がパスワード入力データと登録パスワードデータとの「不一致」を示す場合には、動作制御手段５は、ＰＣカード１の認証ステータスを、準備未完了ステータスとの差異がステータス文字列のみである失敗ステータス（

ステータス文字列“FAILED”で表されるステータス）とし、さらに、パスワードの入力回数が所定回数（例えば３回）未満か否かを判定する。

【００３９】

この判定は、利用側ユニット６から書き込み専用ファイル２ｃへのパスワード入力データの入力回数のカウント値と所定回数を表す予め設定された数値とを比較することで実現されるものであり、この判定結果が「３回未満」を示す場合には、動作制御手段５は、ＰＣカード１の認証ステータスを準備未完了ステータスに戻し、上述した処理を繰り返す。この繰り返し処理において、パスワード入力データは書き込み専用ファイル２ｃに上書きされるか、順に追記される。一方、上記判定結果が「３回以上」を示す場合には、動作制御手段５は、ＰＣカード１の認証ステータスを、利用側ユニット６側からのアクセスを一切受け付けないロックステータス（ステータス文字列“LOCKED”で表されるステータス）とする。

【００４０】

すなわち、動作制御手段５は、所定回数以下のパスワード入力にて正しいパスワードを入力することができたユーザに対してはＰＣカード１の認証ステータスを準備完了ステータスとし、逆に入力することができなかったユーザに対してはＰＣカード１の認証ステータスをロックステータスとする。

【００４１】

③離脱処理

着脱検知手段４によってＰＣカード１の利用側ユニット６からの離脱が検知されると、動作制御手段５は、ＰＣカード１の認証ステータスを準備未完了ステータスとする。また、動作制御手段５は、書き込み専用ファイル２ｃ内のデータを消去するとともに、ＰＣカード１の利用側ユニット６への再装着に備えて、利用側ユニット６から書き込み専用ファイル２ｃへのパスワード入力データの書き込み回数のカウント値をリセットする。なお、本実施形態において、単に「離脱」／「装着」と記載された場合には、「物理的な実際の離脱」／「物理的な実際の装着」を意味する。

【００４２】

④ソフト的離脱・再装着処理

利用側ユニット６側が特定文字列（例えば“DISCONNECT”）を書き込み専用ファイル２ｃに書き込むと、動作制御手段５は、利用側ユニット６に対するＰＣカード１の離脱および再装着をソフト的に行う。具体的には、離脱の検知を省いて上記離脱処理を実行し、さらに装着の検知を省いて上記装着処理を実行する。このソフト的離脱・再装着処理は、マルチユーザ環境やＰＣカード１が装着された利用側ユニット６を長時間報知しなければならない状況などにおいてもセキュリティを確保するために行われる処理である。なお、ＰＣカード１の認証ステータスがロックステータスの場合には上記処理の実行は不可能だが、ロックステータスにあるＰＣカード１を装着した利用側ユニット６を他のユーザが使用したとしても、ＰＣカード１は利用側ユニット６側からのアクセスを一切受け付けないため、セキュリティは確保される。

【００４３】

⑤疑似離脱・再装着処理

ところで、利用側ユニット６において実行されているＯＳが、ディレクトリやファイルのキャッシングを行うＯＳの場合、利用側ユニット６に対してＰＣカード１の離脱・再装着なしに記憶手段２内のディレクトリやファイル名が変更されると、利用側ユニット６において不都合が生じることがある。そこで、本実施形態では、ＰＣカード１の認証ステータスが準備完了ステータスとなったときに、動作制御手段５が利用側ユニット６側へ、ＰＣカード１の離脱・再装着を擬似的に表す信号（以後、疑似着脱・再装着信号）を出力し、キャッシュの不整合を防ぐようにしている。具体的には、動作制御手段５は、所定の接続信号ＣＤ＃１，ＣＤ＃２を一時的に遮断することで、疑似着脱・再装着信号を出力する。

【００４４】

なお、着脱検知手段４は、上記疑似着脱・再装着信号をもってＰＣカード１の実際の着脱を検知してしまうことがないように設定されている。例えば、所定の接続信号ＣＤ＃１，ＣＤ＃２の遮断期間が、疑似着脱・再装着信号に比較して十分に長い場合にのみ実際の着脱と判断するように設定すれば、着脱検知手段４は正確に実際の着脱のみを検知することができる。

【００４５】

Ａ－５：認証動作

次に、上述の構成の認証システムの代表的な認証動作について、図２を参照して説明する。ただし、初期状態として、ＰＣカード１は利用側ユニット６から離脱しており、書き込み専用ファイル２ｃ内のデータは消去されているものとする。また、利用側ユニット６は前述の一般的なＯＳを実行中であるものとする。なお、以下の説明において、処理または動作の主体が省略されている場合には、ＰＣカード１が主体であるものとする。

【００４６】

まず、ＰＣカード１が利用側ユニット６に装着されると、ＰＣカード１の認証ステータスは準備未完了ステータスとなり、利用側ユニット６に対しては、専用ファイル２ｃへの書き込みのみが許容される（ステップＳＡ１）。次いで、ユーザが利用側ユニット６へパスワードを入力することで、このパスワードを表すパスワード入力データが通常のファイルアクセス方法により書き込み専用ファイル２ｃへ書き込まれると（ステップＳＡ２）、動作制御手段５により制御された認証処理手段３により、当該パスワード入力データと登録データファイル２ｄに予め登録された登録パスワードデータとが比較され（ステップＳＡ３）、両者の一致／不一致が判別される（ステップＳＡ４）。

【００４７】

両者が一致した場合（図２では“ＹＥＳ”の場合）、ＰＣカード１の認証ステータスは準備完了ステータスとなる（ステップＳＡ５）。これにより、記憶手段２の汎用メモリ領域２ａ内の各種ディレクトリやファイルが利用側ユニット６側から通常のファイルアクセス方法にて読み出し及び書き込み可能となる。すなわち、パスワード入力データと登録パスワードデータとが一致した場合には、パスワード入力データを入力したユーザはＰＣカード１の正当なユーザとして取り扱われる。

【００４８】

逆に、両者が一致しなかった場合（図２では“ＮＯ”の場合）、ＰＣカード１の認証ステータスは失敗ステータスとなり、ＰＣカード１の装着後のパスワードの入力回数が所定回数（例えば３回（再入力が２回））未満であるか否かが判定

される（ステップＳＡ６）。そして、この判定結果が“ＹＥＳ”であれば、処理はステップＳ1の処理に戻る。以後、正しいパスワードが入力されるか、あるいはパスワード入力回数が所定回数に達するまで、ステップＳＡ１～ＳＡ４，ＳＡ６の処理が繰り返される。

【００４９】

ステップＳＡ１～ＳＡ４，ＳＡ６の処理の繰り返しにおいて、再入力されたパスワード入力データが登録パスワードと一致すれば、ステップＳＡ４の判別結果が“ＹＥＳ”となり、このパスワード入力データを入力したユーザが正当なユーザであると判定され、ＰＣカード１の認証ステータスは準備完了ステータスとなる（ステップＳＡ５）。すなわち、パスワード入力データを入力したユーザはＰＣカード１の正当なユーザとして取り扱われる。

【００５０】

一方、ステップＳＡ１～ＳＡ４，ＳＡ６の処理が繰り返しにおいて、パスワードの入力回数が所定回数に達すると（不一致が所定回連続すると）、ステップＳＡ６の判定結果が“ＮＯ”となる。これにより、ＰＣカード１の認証ステータスはロックステータスとなり、利用側ユニット６からＰＣカード１へのあらゆるアクセスが禁止される（ステップＳＡ７）。すなわち、パスワード入力データを入力したユーザはＰＣカード１の不正なユーザとして取り扱われる。

【００５１】

なお、上記動作の間に、ユーザが利用側ユニット６に対して、書き込み専用ファイル２ｃを通常のファイルアクセス方法により読み出す指示を入力すると、その結果として、ＰＣカード１から利用側ユニット６へ、その時のＰＣカード１の認証ステータスを表すステータス文字列が供給される。このステータス文字列は、例えば、ＯＳが備えている一般的な機能により、利用側ユニット６によりユーザへ通知される。

【００５２】

一方、認証ステータスが上記各種ステータスのいずれであっても、ＰＣカード１が利用側ユニット６から離脱すると、動作制御手段５により、書き込み専用ファイル２ｃ内のデータが消去されるとともに、ＰＣカード１の装着後のパスワー

ドの入力回数のカウント値がリセットされる。また、動作制御手段５により、ＰＣカード１の認証ステータスは準備未完了ステータスとなる。

【００５３】

Ａ－６：まとめ

上述したように、本実施形態においては、通常のメモリへの書き込みと同様に、所定のＯＳの通常のファイルアクセス方法により、利用側ユニット６側から書き込み専用ファイル２ｃへパスワード入力データを書き込み、ＰＣカード１において内部の情報を読み取って比較するだけの簡単な処理によって本人認証を実現することができる。すなわち、利用側ユニット６を何ら変更することなく、ユーザの本人認証を実現することができる。

【００５４】

また、本実施形態においては、利用側ユニット６の接続中であっても、書き込み専用ファイル２ｃに特定文字列を書き込むことで、利用側ユニット６に対してＰＣカード１をソフト的に離脱・装着させることができる。これは、ＰＣカード１の着脱操作を実際に行うことなく、ＰＣカード１の認証ステータスを準備未完了ステータスとすることができることを意味しており、これにより、操作性に優れた認証環境を提供することができる。

【００５５】

さらに、本実施形態においては、利用側ユニット６で実行される所定のＯＳがディレクトリやファイルのキャッシングを行うＯＳであっても、認証成功後に動作制御手段５から利用側ユニット６へ、あたかも利用側ユニット６に対してＰＣカード１を離脱させ装着させたような信号を出力するようにしたので、キャッシュの不整合を解消することができる。

【００５６】

Ａ－７：補足

なお、本実施形態においては、パスワード入力データが登録パスワードデータと一致するか否かをもって正当なユーザであるか否かを判別するようにしたが、パスワード入力データが所定の条件を満たした場合に、当該データを入力したユーザが正当なユーザであると判別するようにしてもよい。例えば、パスワード入

力データがＰＣカード１に予め登録されたデータと所定の関係にある場合に正当なユーザであると判別するようにしてもよい。

〔００５７〕

また、ＰＣカードはＡＴＡ（AT Attachment）　ＰＣカードであってもよく、この場合には、着脱検知手段４において、マイクロコントローラ内部のＡＴＡステータス・レジスタのメディア交換ビット（ＭＣ）を監視して着脱を検知するようにし、動作制御手段５において、当該メディア交換ビットを制御してＰＣカード１の疑似離脱・再装着信号を利用側ユニット６へ出力するようにすることになる。なお、着脱検知手段４はハードウェア的なスイッチであってもよい。

〔００５８〕

なお、ＰＣカードのマイクロコントローラは外部インタフェースを介して利用側ユニット６から電力の供給を受けてもよいし、揮発性の半導体メモリのバックアップ電源から電力の供給を受けてもよい。ただし、当該マイクロコントローラが利用側ユニット６から供給される電力のみによって駆動される場合、ＰＣカードの利用側ユニット６からの離脱時にはマイクロコントローラは作動を停止してしまうため、ＰＣカードの構成を変形する必要がある。以下、その変形の一例（変形例）について説明する。

〔００５９〕

Ａ－８：変形例

図３は本変形例によるＰＣカード１１を用いた認証システムの構成を示すブロック図である。本変形例によるＰＣカード１１が前述のＰＣカード１とハードウェア的に異なる点は、マイクロコントローラが利用側ユニット６から供給される電力のみによって駆動される点と、不揮発性のメモリの他にバッテリバックアップされていない揮発性の半導体メモリを備えている点である。

〔００６０〕

また、本変形例によるＰＣカード１１がＰＣカード１と機能的に異なる点は、着脱検知手段４を持たない点と、記憶手段２及び動作制御手段５に代えて記憶手段１２及び動作制御手段１５を備えた点である。なお、ＰＣカード１１が着脱検知手段４を持たない理由は以下の通りである。

[理由1] 利用側ユニット６へのＰＣカード１１の装着時にマイクロコントローラが作動を開始することから、このことを利用すればＰＣカード１１の装着を検知する必要はない。

[理由２] 利用側ユニット６からのＰＣカード１１の離脱時に不揮発性メモリの記憶内容は保持されないことから、このことを利用すればＰＣカード１１の離脱を検知する必要はない。

【００６１】

記憶手段１２が記憶手段２と異なる点は、揮発性メモリを有し、この揮発性メモリに書き込み専用ファイル２ｃを格納する点である。すなわち、書き込み専用ファイル２ｃはＰＣカード１１が利用側ユニット６に装着されている場合にのみ存在し、ＰＣカード１１の利用側ユニット６からの離脱時に消失する。

【００６２】

動作制御手段１５が動作制御手段５と異なる点は、着脱検知手段４の検知結果ではなく、自手段（マイクロコントローラ）の動作状態に応じて各種処理を行う点である。これら各種の処理において、動作制御手段５による処理と異なる点は、自手段の動作開始時点をＰＣカード１１が利用側ユニット６へ装着された時点と判断し、揮発性メモリ上に書き込み専用ファイル２ｃを生成し、前述の装着処理を行う点である。なお、利用側ユニット６からのＰＣカード１１の離脱時には動作制御手段１５が作動を停止するため、動作制御手段１５は前述の離脱処理を行う機能を備えていない。

【００６３】

このような構成のＰＣカード１１を用いた代表的な認証処理の流れを図４に示す。この図において図２と共通する処理には同一の符号を付し、その説明を省略する。図４から明らかなように、本変形例によるＰＣカード１１の装着時（すなわち、マイクロコントローラの作動開始時）には、まず、書き込み専用ファイル２ｃが記憶手段１２の揮発性メモリ上に生成され（ステップＳＢ１）、以後、図２に示す処理が行われる。一方、本変形例によるＰＣカード１１では、利用側ユニット６からＰＣカード１１が離脱すると、揮発性メモリへの電力供給が遮断され、揮発性メモリ上の書き込み専用ファイル２ｃは消失する。

【００６４】

このように、本変形例によるＰＣカード１１によれば、着脱検知手段４を備えずとも、ＰＣカード１と同様の効果を得ることができる。

【００６５】

Ｂ．第２実施形態

次に、本発明の第２実施形態について説明する。

【００６６】

Ｂ－１．基本的技術思想

まず、本実施形態において採用された基本的技術思想について説明する。

本実施形態では、利用側ユニットに固定的に内蔵されたメモリデバイスを対象としており、メモリデバイス内にユーザデータを記憶するための汎用メモリ領域と本人認証および自デバイスの動作の制御を行う手段とを設けている。そして、本実施形態に係るメモリデバイスは、利用側ユニットへのユーザのログイン時には、自デバイスの認証ステータスを、自デバイス内の書き込み専用ファイルへの書き込みのみを利用側ユニットに対して許容する準備未完了ステータスとし、この書き込み専用ファイルにパスワードとして利用側ユニット側から書き込まれたデータとメモリデバイス内に予め登録されたデータ（利用側ユニットから読み出し不可能に格納されたデータ）とを比較し、両者が一致した場合にのみ、自デバイスの認証ステータスを、利用側ユニット側から汎用メモリ領域へのアクセスを許容する準備完了ステータスへ変更するようにしている。

【００６７】

Ｂ－２．システム構成

まず、本実施形態に係るメモリデバイスを用いた認証システムの構成について説明する。図５は本実施形態に係るメモリデバイスを用いた認証システムの構成を示すブロック図であり、この図において、図１（又は図３）と共通する部分には同一の符号を付し、その説明を省略する。

【００６８】

図５において、２１はメモリデバイスとして機能するハードディスク装置、２６はハードディスク装置２１が固定的に接続された利用側ユニットであり、ハー

ドディスク装置２１をメモリデバイスとして利用する。２７はハードディスク装置２１と利用側ユニット２６とから構成される情報処理装置である。情報処理装置２７は、ユーザのログイン／ログアウトを管理可能な一般的なＯＳを搭載し、かつハードディスク装置２１をメモリデバイスとして利用可能な据置型コンピュータである。なお、この条件さえ満たせば、他の電子機器（携帯型のコンピュータや各種セットトップボックス等）を情報処理装置２７としてよいことは言うまでもない。

【００６９】

Ｂ－３：ハードウェア構成

次に、ハードディスク装置１１のハードウェア構成について説明する。

図示を略すが、ハードディスク装置２１は、データを磁気記憶する不揮発性の記憶媒体を有するハードディスクドライブと、当該ドライブに対してデータの読み出し／書き込み等を行うコントローラと、このコントローラを利用側ユニット２６に接続するためのインタフェースとを備えている。また、コントローラはインタフェースを介して利用側ユニット２６とデータの授受を行うとともに、後述する本人認証処理を行う。なお、ハードディスク装置２１は電源専用ラインを介して利用側ユニット２６から電力の供給を受ける。

【００７０】

Ｂ－５：機能構成

次に、上記ハードウェア構成上に実現されるハードディスク装置２１の機能構成について説明する。ただし、第１実施形態における「ＰＣカード１」を「ハードディスク装置２１」に変更すれば足りる部分については、容易に推定可能であるため、その説明を省略する。

【００７１】

図５に示すように、ハードディスク装置２１は、ハードディスクドライブから構成された記憶手段２、コントローラにより実現される認証処理手段３、コントローラ及びインタフェースから構成されるログイン／ログアウト検知手段（ログイン検知手段）２４、コントローラ及びインタフェースから構成される動作制御手段２５を有する。

【００７２】

ログイン／ログアウト検知手段２４は、情報処理装置２７のＯＳからハードディスク装置２１を含む内蔵機器（および周辺機器）へ通知されるログイン／ログアウトの情報に基づいて、情報処理装置２７に対するユーザのログイン／ログアウトを検知し、ログイン時およびログアウト時に、その旨を動作制御手段２５へ供給する。

【００７３】

動作制御手段２５が図１の動作制御手段５と異なる点は、「装着処理」及び「離脱処理」に代えて「ログイン処理」及び「ログアウト処理」を行う点と、「ソフト的離脱・再装着処理」及び「疑似離脱・再装着処理」のための機能を備えていない点である。なお、「ソフト的離脱・再装着処理」のための機能を備えていないのは、ユーザがログアウト及び再ログイン操作を行うことによって十分に高いセキュリティを確保できるためである。また、「疑似離脱・再装着処理」のための機能を備えていないのは、その必要性がないためである。

【００７４】

①ログイン処理

動作制御手段２５によるログイン処理が動作制御手段５による装着処理と異なる点は契機のみであり、ログイン／ログアウト検知手段２４によってユーザのログインが検知されると、動作制御手段２５はハードディスク２１の認証ステータスを、利用側ユニット２６からの書き込み専用ファイル２ｃへの書き込みのみを許容する準備未完了ステータスとするとともに、利用側ユニット２６側から書き込み専用ファイル２ｃへのパスワード入力データの書き込み回数のカウントを開始する。

【００７５】

②ログアウト処理

動作制御手段２５によるログアウト処理が動作制御手段５による離脱処理と異なる点は契機のみであり、ログイン／ログアウト検知手段２４によってユーザのログアウトが検知されると、動作制御手段２５はハードディスク装置２１の認証ステータスを準備未完了ステータスとする。また、動作制御手段２５は、書き込

み専用ファイル２ｃ内のデータを消去するとともに、ユーザのログインに備えて、利用側ユニット２６から書き込み専用ファイル２ｃへのパスワード入力データの書き込み回数のカウント値をリセットする。

【００７６】

Ｂ－５：認証動作

上述の構成の情報処理装置２７において、ユーザが情報処理装置２７にログインすると、このことがログイン／ログアウト検知手段２４によって検知され、動作制御手段２５においてログイン処理が行われる。前述のように、ログイン処理は、その契機を除いてＰＣカード１の装着処理と同一（図２と同一）であることから、以降の説明を省略する。

【００７７】

一方、情報処理装置２７に対してユーザがログアウトすると、このことがログイン／ログアウト検知手段２４によって検知され、動作制御手段２５においてログアウト処理が行われる。前述のように、ログアウト処理は、その契機を除いてＰＣカード１の離脱処理と同一であることから、以降の説明を省略する。

【００７８】

Ｂ－６：まとめ

上述したように、本実施形態においては、演算処理装置２７に固定的に内蔵されたハードディスク装置２１について、第１実施形態におけるＰＣカード１と同様に、高いセキュリティを容易に確保することができる。

【００７９】

Ｂ－７：補足

なお、本実施形態においてはハードディスク装置を例に挙げたが、これに代えて、半導体ディスク等の他の記憶装置を用いてもよい。

【００８０】

Ｃ：全体の補足

なお、本発明は上述した各実施形態および変形例の具体的な構成に限定されるものではないし、これらの実施形態および変形例に限定されるものでもない。例えば、第１実施形態に係るメモリデバイスにおいて、ユーザのログイン時に本人

認証を行うようにしてもよい。さらに、ユーザを識別するための情報は、ユーザを一意に特定可能な情報であればよく、パスワードに限定されるものではない。ただし、利用側ユニットの改造や変更を要するものであってはならない。また、本発明は記憶専用のメモリデバイスに限定されるものではなく、通信機能（例えば有線もしくは無線モデムの機能）を併有するメモリデバイスであってもよい。

【００８１】

【発明の効果】

本発明によれば、利用側ユニット側から汎用メモリへのアクセス方法と同様の通常のファイルアクセス方法にて書き込み可能な書き込み専用領域が設けられており、この書き込み専用領域に利用側ユニット側から書き込まれた入力データと予め登録された登録データとが所定の関係（例えば一致関係）にあるか否かに基づいてユーザの本人性の認証が行われ、本人性が正しく認証された場合に利用側ユニット側からの汎用記憶部へのアクセスが可能となる。この構成によれば、通常のファイルアクセス方法によるファイルアクセスが可能な利用側ユニットを何ら変更することなく、本人認証を実現することができる。すなわち、高いセキュリティのメモリデバイスを容易に実現することができる。

【００８２】

また、利用側ユニットへのメモリデバイスの装着時や利用側ユニットに対するユーザのログイン時に本人認証を行うようにすれば、メモリデバイスへの不正アクセスを確実に排除することができる。

【００８３】

さらに、書き込み専用領域への所定回数までの書き込みを許容し、各々の書き込みにおいて認証処理を行うようにすれば、正当なユーザによるアクセスが誤入力等によって排除されてしまうという事態を回避することができる。また、所定回数以下の書き込みにおいても本人性を認証できない場合に利用側ユニット側から書き込み専用領域への書き込みを禁止するようにすれば、より高いセキュリティを確保することができる。

【００８４】

また、利用側ユニットへの自デバイスの再装着時や利用側ユニットに対するユ

ーザの再ログイン時に、自デバイスの状態を、利用側ユニット側から前記書き込み専用領域への書き込み以外のアクセスを禁止した状態としておくことにより、より高いセキュリティを確保することができる。

【００８５】

さらに、利用側ユニットに対する自デバイスの着脱状態の変化を擬似的に表わす信号を利用側ユニットへ出力するようにすれば、メモリデバイスの着脱操作を行わないことによる不都合（例えば、ディレクトリやファイル名をキャッシングするオペレーティングシステムにおいて発生する不都合）を回避することができる。

【００８６】

また、特定の指示に応じて、自デバイスの状態を、利用側ユニット側から書き込み専用領域への書き込みのみを許容し、かつ装着検知手段（ログイン検知手段）によって利用側ユニットへの自デバイスの装着（ユーザのログイン）が検知された状態とするようにすれば、メモリデバイスを実際に離脱・再装着することなく、認証処理を開始することができる。すなわち、ユーザにかかる負担を軽減することができる。

【００８７】

さらに、利用側ユニット側から書き込み専用領域を通常のファイルアクセス方法にて読み出す要求を受け取ると、自デバイスの状態を表す情報を返送するようにしてもよい。これにより、利用側ユニット側では、通常のファイルアクセス方法にてメモリデバイスの状態を知ることができる。

【図面の簡単な説明】

【図１】　本発明の第１実施形態に係るメモリデバイスを用いた認証システムの構成を示すブロック図である。

【図２】　同メモリデバイスにおける代表的な認証処理の流れを示すフローチャートである。

【図３】　本発明の第１実施形態の変形例によるＰＣカード１１を用いた認証システムの構成を示すブロック図である。

【図４】　同ＰＣカード１１を用いた代表的な認証処理の流れを示すフロー

チャートである。

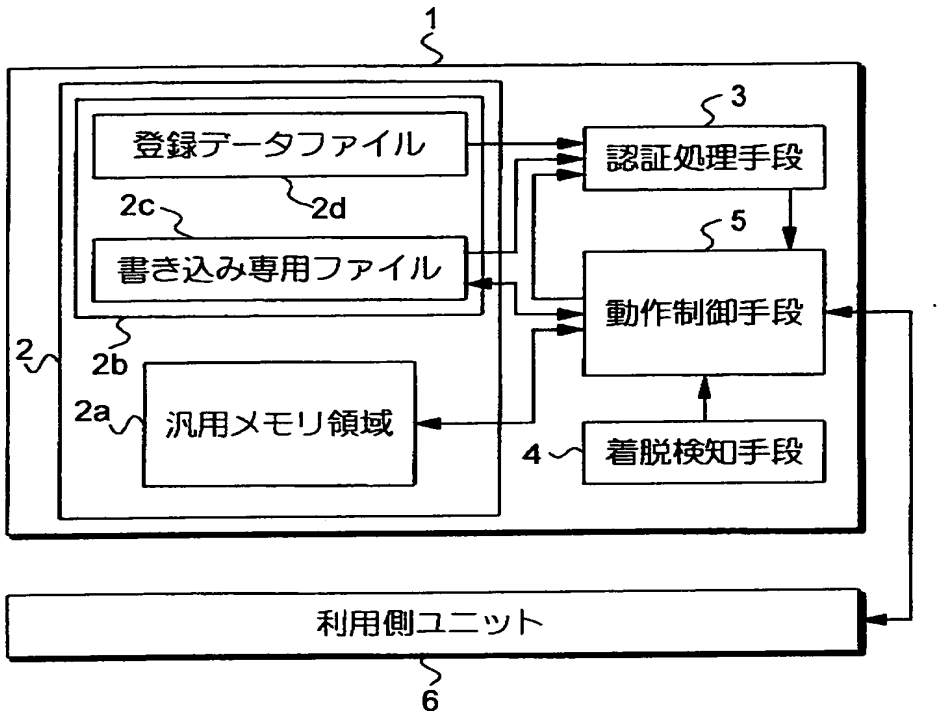
【図５】　本発明の第２実施形態に係るメモリデバイスを用いた認証システムの構成を示すブロック図である。

【符号の説明】

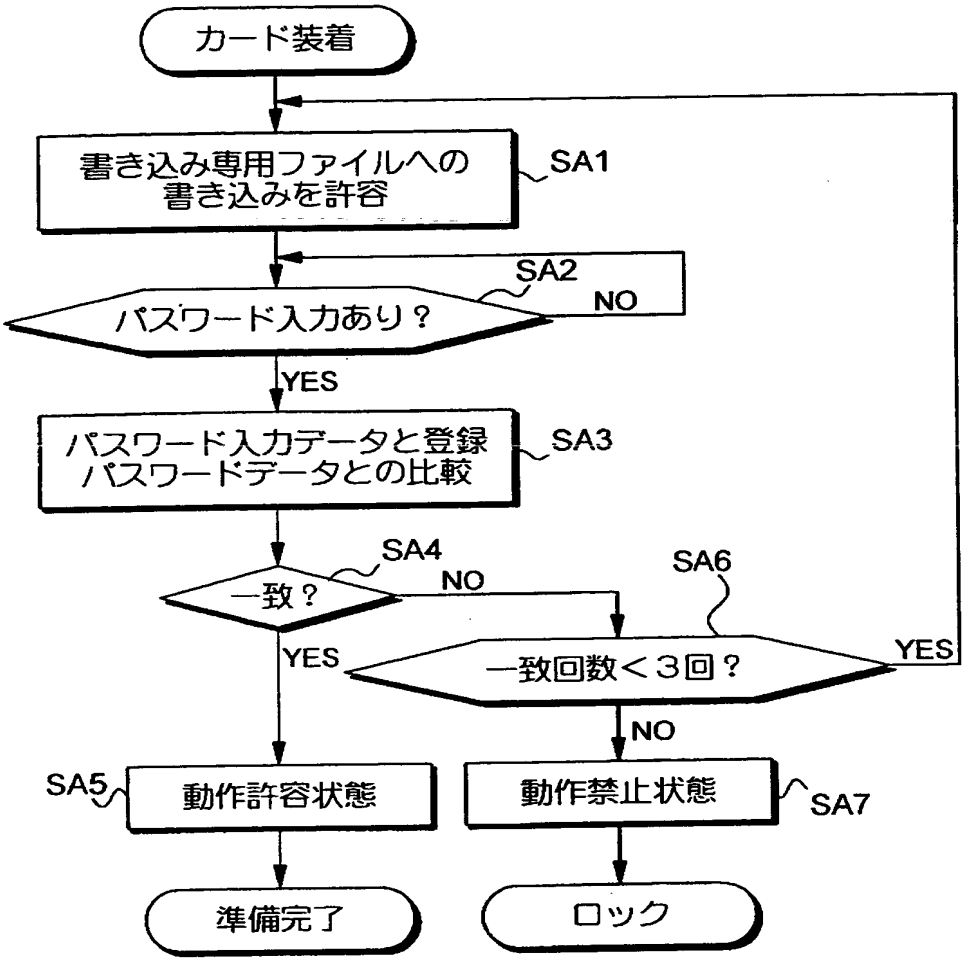
１，１１	ＰＣカード
２，１２	記憶手段
２ａ	汎用メモリ領域
２ｂ，１２ｂ	認証用データ格納領域
２ｃ	書き込み専用ファイル
２ｄ	登録データファイル
３	認証処理手段
４	着脱検知手段
５，１５，２５	動作制御手段
６，２６	利用側ユニット
２４	ログイン／ログアウト検知手段
２７	情報処理装置

【書類名】　図面

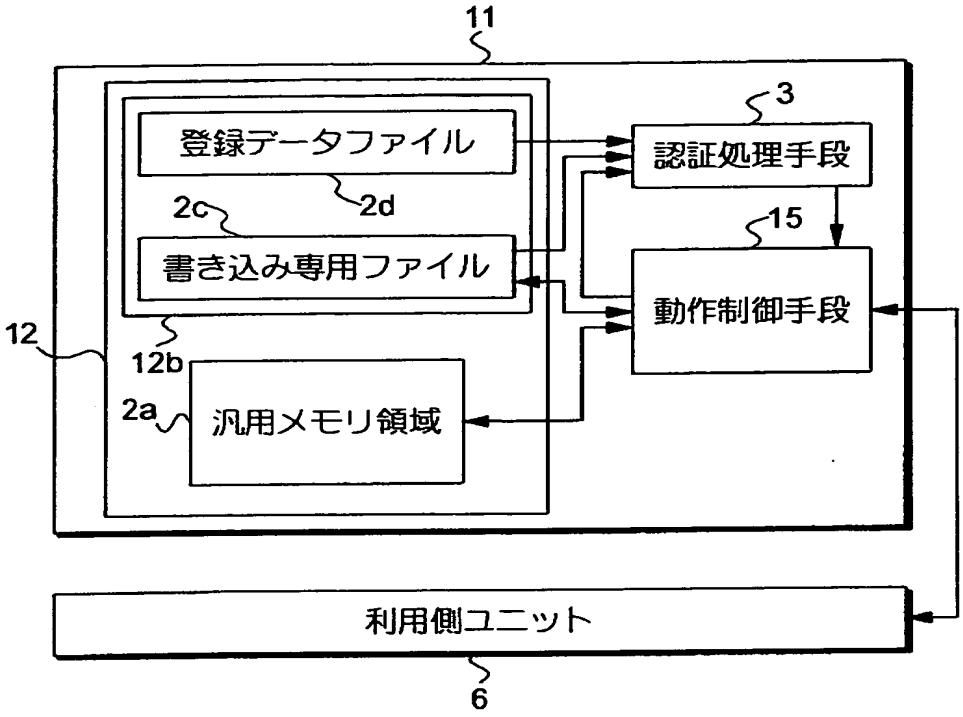
【図１】


1
登録データファイル
2d
2c
書き込み専用ファイル
2
2b
2a
汎用メモリ領域
3
認証処理手段
5
動作制御手段
4
着脱検知手段
利用側ユニット
6

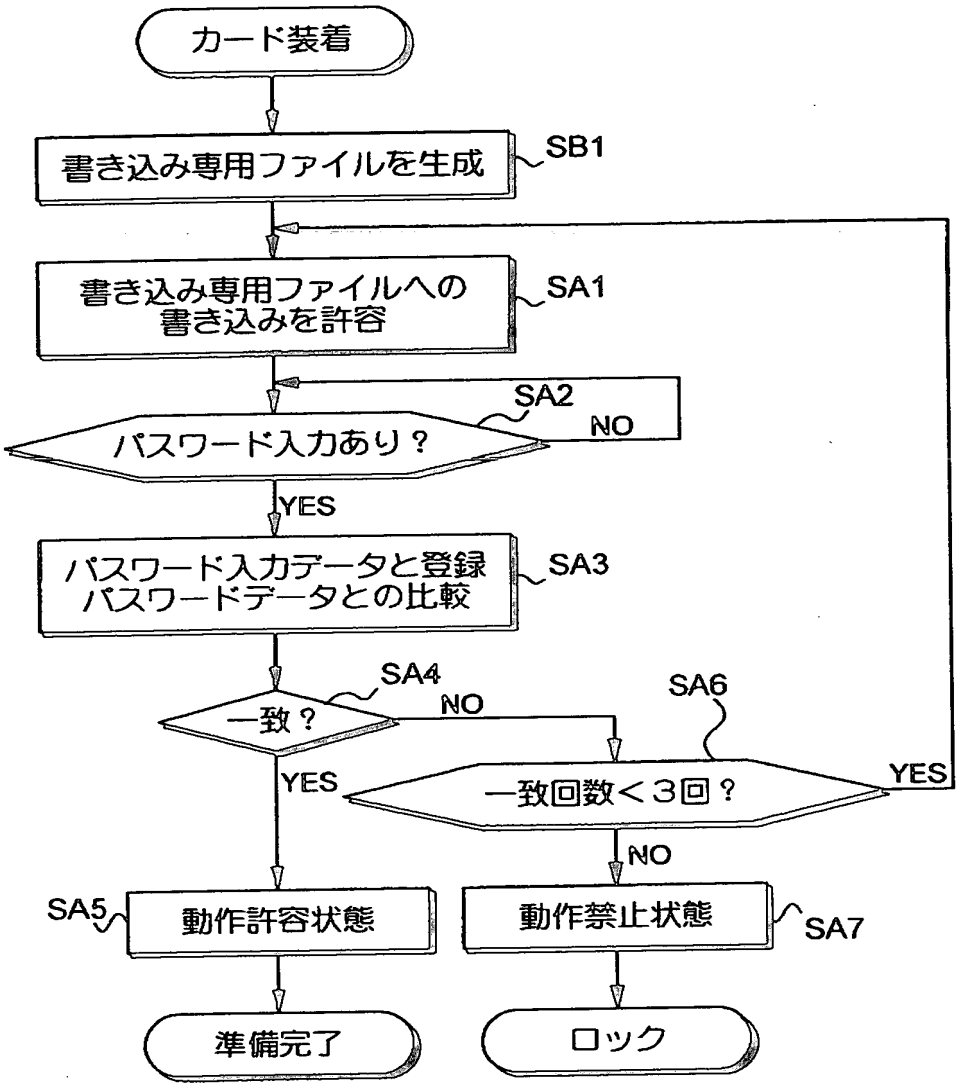
【図２】


カード装着
書き込み専用ファイルへの書き込みを許容
SA1
SA2
パスワード入力あり？
NO
YES
パスワード入力データと登録パスワードデータとの比較
SA3
SA4
一致？
NO
SA6
YES
一致回数＜３回？
YES
NO
SA5
動作許容状態
動作禁止状態
SA7
準備完了
ロック

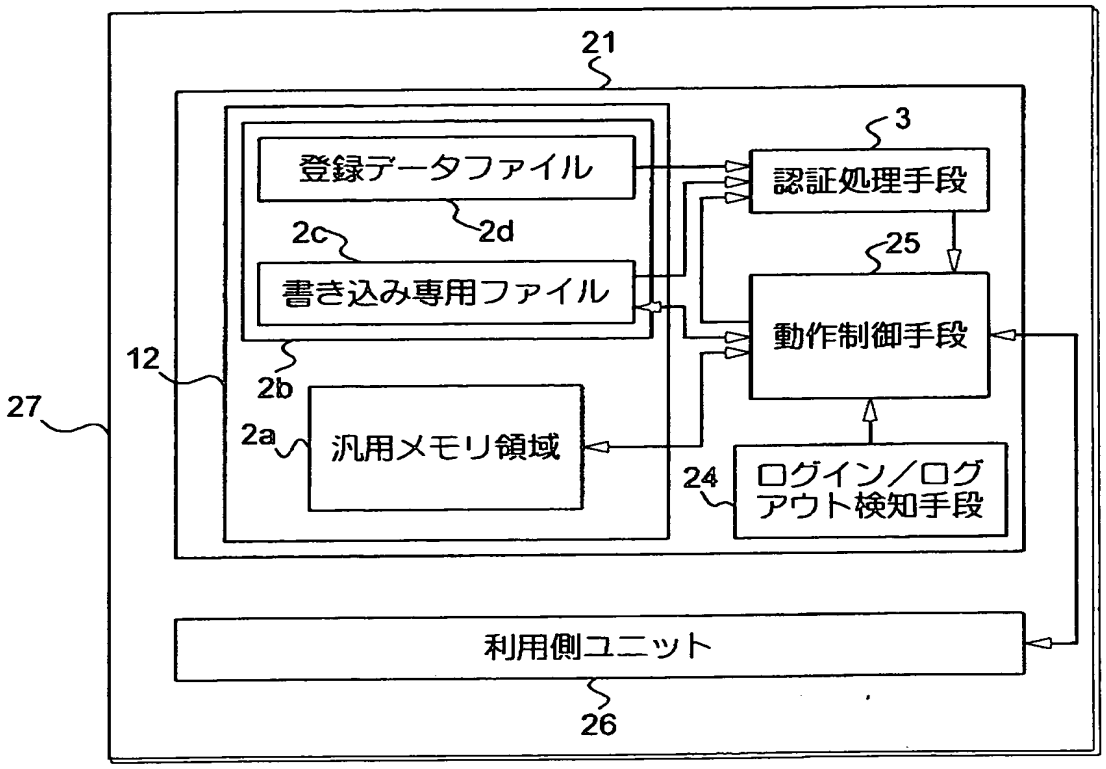
【図３】


11
3
登録データファイル
認証処理手段
2d
2c
15
書き込み専用ファイル
動作制御手段
12
12b
2a
汎用メモリ領域
利用側ユニット
6

【図４】


カード装着
書き込み専用ファイルを生成
SB1
書き込み専用ファイルへの
書き込みを許容
SA1
SA2
NO
パスワード入力あり？
YES
パスワード入力データと登録
パスワードデータとの比較
SA3
SA4
NO
一致？
SA6
YES
一致回数＜３回？
YES
NO
SA5
動作許容状態
動作禁止状態
SA7
準備完了
ロック

【図５】


21
3
登録データファイル
認証処理手段
2d
2c
25
書き込み専用ファイル
動作制御手段
12
2b
27
2a
汎用メモリ領域
24
ログイン／ログアウト検知手段
利用側ユニット
26

【書類名】　　要約書

【要約】

【課題】　自デバイスが装着される利用側ユニットに何ら変更を加えることなくユーザの本人認証を行うことができるメモリデバイスを提供する。

【解決手段】　利用側ユニット６側から汎用メモリ領域２ａへのファイルアクセスと同様の通常のファイルアクセス方法で書き込み可能な書き込み専用ファイル２ｃを記憶手段２に設け、着脱検知手段４により利用側ユニット６への自デバイスの装着が検知され、かつ利用側ユニット６側から書き込み専用ファイル２ｃへパスワード入力データが書き込まれると、このパスワード入力データと予め登録された登録データとを認証処理手段３が比較する。ここで両者が一致した場合には、動作制御手段５が、利用側ユニット６側から汎用メモリ領域２ａへのアクセスを許容する。

【選択図】　　図１

出証特２０００－３０５７５２１

【書類名】　手続補正書

【提出日】　平成12年 3月14日

【あて先】　特許庁長官　殿

【事件の表示】

【出願番号】　特願2000- 59369

【補正をする者】

【識別番号】　392026693

【氏名又は名称】　エヌ・ティ・ティ移動通信網株式会社

【代理人】

【識別番号】　100098084

【弁理士】

【氏名又は名称】　川▲崎▼　研二

【電話番号】　03-3242-5481

【手続補正　1】

【補正対象書類名】　特許願

【補正対象項目名】　発明者

【補正方法】　変更

【補正の内容】

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　エヌ・ティ・ティ移動通信網株式会社内

【氏名】　福本　雅朗

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　エヌ・ティ・ティ移動通信網株式会社内

【氏名】　杉村　利明

【その他】　平成１２年３月３日付出願の特許２０００－５９３６９号の特許出願の発明者の住所を「東京都千代田区永田町二丁目１１番１号　エヌ・ティ・ティ移動通信網株式会

社内」と記するところを誤って「東京都港区虎ノ門二丁目１０番１号　エヌ・ティ・ティ移動通信網株式会社内」として出願してしまいましたので、上記住所の誤記を訂正いたしたく本書を提出致しますので、宜しくお願い申し上げます。

【プルーフの要否】　要

出願人履歴情報

識別番号　〔３９２０２６６９３〕

１．変更年月日　１９９２年　８月２１日
［変更理由］　新規登録
住　所　東京都港区虎ノ門二丁目１０番１号
氏　名　エヌ・ティ・ティ移動通信網株式会社

２．変更年月日　２０００年　５月１９日
［変更理由］　名称変更
住　所　東京都千代田区永田町二丁目１１番１号
氏　名　株式会社エヌ・ティ・ティ・ドコモ